

Serial No. 09/741,251

RD-27,606

Remarks

Applicant carefully considered the Office Action mailed on July 14, 2004. Claims 1-101 are pending in the present patent application. Of the pending claims, the Examiner rejected claims 1-101. In response to the Office Action, Applicant amended the specification to overcome the objection to the drawings under 37 CFR 1.84(p)(5). No new matter has been added. In view of the above amendment and the following remarks, Applicant requests further examination and reconsideration of the present patent application.

The Examiner rejected claims 1-101 under 35 USC § 102(e) as being anticipated by Lloyd et al. (US Patent No. 6,219,790). Applicant respectfully traverses the § 102(e) rejection of the present patent application and submits that Lloyd et al. (hereinafter Lloyd) does not anticipate the claimed invention.

In one form or another, independent claims 1, 10, 27, 54, 62, 92 and 100 of the present invention recite a gateway device for securely managing activities between at least one device and at least one service provider. The gateway device comprises an authenticator that authenticates the identity of the at least one service provider and the at least one device; an access authorizer that permits the at least one service provider to interact with the at least one device; and an activity manager, responsive to the access authorizer and the authenticator, that manages the activities occurring between the at least one service provider and the at least one device.

Independent claims 19, 70 and 101 of the present invention, in one form or another, recite a gateway device for securely managing activities between at least one device and at least one service provider. The gateway device comprises a request handler that receives activity requests from the at least one service provider and the at least one device; an authenticator that authenticates the identity of the at least one service provider and the at least one device; an access authorizer that permits the at least one service provider to interact with the at least one device; an activity manager that manages the activity requests occurring between the at least one service provider and the at least one device; and a response component, responsive to the request handler, the authenticator, the access authorizer and the activity manager, that receives activity responses from the at least one service provider and the at least one device.

Serial No. 09/741,251

RD-27,606

Independent claim 26 of the present invention recites a gateway device for securely managing activities between at least one device and at least one service provider. The gateway device comprises a request handler that receives activity requests from the at least one service provider and the at least one device; an authenticator that authenticates the identity of the at least one service provider and the at least one device; an access authorizer that permits the at least one service provider to interact with the at least one device; an activity manager that manages the activity requests occurring between the at least one service provider and the at least one device; a data format translator that translates the format of data transmitted and received by the at least one service provider and the at least one device during the activities; and a response component, responsive to the request handler, the authenticator, the access authorizer, the activity manager, and the data format translator that receives activity responses from the at least one service provider and the at least one device.

Independent claims 36 and 76 of the present invention, in one form or another, recite a system for securely providing services between a first site and a second site. The system comprises at least one appliance linked in a first network at the first site and a service provider linked to the at least one appliance in a second network at the second site. The system further comprises a gateway device that securely manages the services provided between the at least one appliance and the service provider. The gateway device comprises an authenticator that authenticates the identity of the service provider and the at least one appliance. The gateway device further comprises an access authorizer that permits the service provider to interact with the at least one appliance, and a service manager, responsive to the authenticator and the access authorizer, that manages the services provided between the service provider and the at least one appliance.

In addition, independent claims 45 and 84 of the present invention, in one form or another, recite a system for securely providing remote monitoring and diagnostics. The system comprises at least one device linked to a first network and a service provider linked to the at least one device in a second network. The system further comprises a gateway device that securely manages remote monitoring and diagnostic activities between the at least one device and the service provider. The gateway device comprises an authenticator that authenticates the identity of the service provider and the at least one device. The gateway device further comprises an access authorizer that permits the service provider to interact with the at least one device; and an activity manager, responsive to the authenticator and access authorizer, that manage the remote monitoring and diagnostic activities provided between the service provider and the at least one device.

Serial No. 09/741,251

RD-27,606

Lloyd does not disclose a gateway device for securely managing activities between a device and a service provider, wherein the gateway device comprises an authenticator that authenticates the identity of the service provider and the device; an access authorizer that permits the service provider to interact with the device; and an activity manager, responsive to the access authorizer and the authenticator, that manages the activities occurring between the service provider and the device. The Examiner referenced col. 3, lines 23-30, as being relevant to a gateway device including an authenticator. Applicant carefully reviewed this section noted by the Examiner and submits that it does not anticipate the claimed limitation of a gateway device including an authenticator that authenticates the identity of a service provider and a device. Instead, the material in col. 3, lines 23-30 relates to a mechanism for authenticating and authorizing user access to a computer network by determining if the login information provided by a user matches information stored in a user record. The teaching in this section is not analogous to the claimed limitation because there is no mention of a gateway device for securely managing activities between a device and a service provider, wherein the gateway device includes an authenticator to authenticate the identity of a service provider. Lloyd does not teach this limitation because it is not concerned with a gateway device for securely managing activities between devices and providers. Instead, Lloyd is only interested in the creation of a single database for maintaining accounting information and user authentication and authorization information. Further, Lloyd is concerned with the creation of a centralized general-purpose authentication, authorization and accounting (AAA) server for authorizing user access to a computer network.

The Examiner also referenced col. 3, lines 31-34 as being relevant to an access authorizer. Applicant carefully reviewed this section noted by the Examiner and submits that it does not anticipate the claimed limitation of a gateway device that includes an access authorizer, wherein the access authorizer permits a service provider to interact with a device. Instead, the material in col. 3, lines 31-34 relates to determining if a user is authorized to access a requested service. The teaching in this section is not analogous to the claimed limitation because there is no mention of a gateway device that includes an access authorizer to permit a service provider to interact with a device. Lloyd does not teach this limitation because it is not concerned with a gateway device that includes an access authorizer to permit a service provider to interact with a device.

Serial No. 09/741,251

RD-27,606

The Examiner also referenced col. 4, lines 48-50 and col. 13 lines 2-21 as being relevant to an activity manager. Applicant carefully reviewed this section noted by the Examiner and submits that it does not anticipate the claimed limitation of an activity manager responsive to the access authorizer and the authenticator that manages the activities occurring between the service provider and the device. Instead, this section relates to security and accounting services performed by the authentication, authorization and accounting (AAA) server such as providing information and reports to users for purposes such as accounting. The teaching in this section is not analogous to the claimed limitation because there is no mention of a gateway device that includes an activity manager responsive to the access authorizer and the authenticator that manages the activities occurring between the service provider and the device. Lloyd does not teach this limitation because it is not concerned with a gateway device that includes an activity manager.

The Examiner referenced col. 5, lines 59-64 as being relevant to a request handler that receives activity requests from the service provider and the device. Applicant carefully reviewed this section noted by the Examiner and submits that it does not anticipate the claimed limitation of a request handler that receives activity requests from the service provider and the device. Instead, this section relates to receiving an authentication request to validate a user request. The teaching in this section is not analogous to the claimed limitation because there is no mention of a gateway device that includes a request handler that receives activity requests from the service provider and the device. Lloyd does not teach this limitation because it is not concerned with a gateway device that includes a request handler.

The Examiner referenced col. 3, lines 8-9 as being relevant to a data format translator that translates the format of data transmitted and received by the service provider and the device during the activities. Applicant carefully reviewed this section noted by the Examiner and submits that it does not anticipate the claimed limitation of a data format translator that translates the format of data transmitted and received by the service provider and the device during activities. Instead, this section relates to the translation of client requests into a standard internal format. The teaching in this section is not analogous to the claimed limitation because there is no mention of a gateway device that includes a data format translator that translates the format of data transmitted and received by the service provider and the device during the activities. The data format translator of the present invention enables a device and a service provider to

Serial No. 09/741,251

RD-27,606

exchange data that are in different formats. Lloyd does not teach this limitation because it is not concerned with a gateway device that includes a data format translator that translates the format of data transmitted and received by the service provider and the device.

The Examiner referenced col. 5, lines 38-40 as being relevant to a system including an appliance in a first network (Figure 1, workstation 128) and a service provider in a second network (Figure 1, network 102). Applicant carefully reviewed this section noted by the Examiner and submits that it does not anticipate the claimed limitation of a system for securely providing services between a first site and a second site comprising an appliance linked in a first network at the first site and a service provider linked to the appliance in a second network at the second site. Instead, this section relates to a user requesting access to a network from a workstation connected to a network server access (NAS) device. The teaching in this section is not analogous to the claimed limitation because there is no mention of a system including an appliance in a first network and a service provider in a second network. Lloyd does not teach this limitation because it is not concerned with a system for securely providing services between a first site and a second site comprising an appliance linked in a first network at the first site and a service provider linked to the appliance in a second network at the second site. Instead, Lloyd is only interested in the creation of a single database for maintaining accounting information and user authentication and authorization information. Further Lloyd is concerned with the creation of a centralized general-purpose authentication, authorization and accounting (AAA) server for authorizing user access to a computer network.

In addition, Lloyd does not disclose a system for securely providing remote monitoring and diagnostics as recited in claims 45 and 84 of the present patent application. Claims 45 and 84 also recite limitations similar to the above noted independent claims, but are set out in a remote monitoring and diagnostics embodiment.

In view of the above-noted distinctions, Applicant submits that the claimed invention as recited in independent claims 1, 10, 19, 26, 27, 36, 45, 54, 62, 70, 76, 84, 92, 100 and 101 is patentably distinguishable over Lloyd. Accordingly, Applicant submits that Lloyd does not anticipate claims 1, 10, 19, 26, 27, 36, 45, 54, 62, 70, 76, 84, 92, 100 and 101.

Claims 2-9, 11-18, 20-25, 28-35, 37-44, 46-53, 55-61, 63-69, 71-75, 77-83, 85-91 and 93-99 depend directly or indirectly from now presumably allowable claims 1, 10, 19, 26, 27, 36,

Serial No. 09/741,251

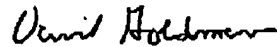
RD-27,606

45, 54, 62, 70, 76, 84, 92, 100 and 101, respectively, and thus are allowable by dependency. Accordingly, Applicant requests that the Examiner reconsider and remove the §102(e) rejection of claims 1-101 under Lloyd.

In view of the foregoing remarks, Applicant requests that the Examiner reconsider this application and allow claims 1-101.

If the Examiner has any questions regarding the present patent application, the Examiner can call Applicant's attorney, David Goldman, at telephone number (518)-387-5927 or (518)-387-5903.

Respectfully submitted,



David C. Goldman

Attorney for Applicant

Registration No. 34,336

Schenectady, New York

Dated: September 13, 2004